UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,557	07/26/2001	Donald E. Duval	BRCMP009	9224

7590 07/26/2005

CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/916,557	DUVAL, DONALD E.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in replay to an amendment filed on May 16, 2005.

   Claims 1,3,5,11-12 and 22 have been amended and claims 1-22 are pending in the application.

2. Examiner has acknowledged and consequently withdraws the objection previously made to the specification due to some informalities as all the objection are properly corrected by the applicant.

3. Examiner has also acknowledge and consequently withdraws the 112 rejection previously made to some of the claims as all of them are properly corrected by the applicant.

Response to Argument

4. Applicant's remark/arguments filed on May 16, 2005 have been fully considered but they are not persuasive.

   Applicants **amended** the independent claims 1 **and 11**, and added a new limitation which was not part of the original claims. Applicant amended claim 1 and changed/added the previous limitation. The amended limitation part of claim 1 recites the following, "...an encryption accelerator ... including a state memory... wherein the state memory is initialized with an incrementing pattern without loading the incrementing pattern from an external memory." And the amended limitation of claim 11 recites the following new limitation, " Storing of an incrementing pattern in the state memory without loading the incrementing pattern from an external memory,

   Applicant's argument has been considered fully.

Applicant's first argument is regarding the independent claims 1 and 11

Applicant's argument is based on the amended claims and argued that the newly added limitation shown above which is added on the independent claims is not suggested/discussed by **the references** on the record, namely the combination of **Vano and Schneier**.

Applicants wrote the following in support of his argument

" As acknowledged by the Examiner, Vano fails to disclose an encryption accelerator that stores an incrementing pattern in the state memory array. The examiner, however relies on the disclosure in Schneier to make for this deficiency. Specifically, the Examiner relies on page 397-398 of Schneier which discloses the use of an 8* 8 S-box: S1, ..., S255. The S-box is initialized by filling it linearly as follows: s0=0, s1=1, ..., s255=255.

However, nothing in schneier teaches or suggests that a "state Memory is initialized with an incrementing pattern without loading the incrementing patten from an external memory" as is recited in claim 1. In fact, there is nothing in Schneier or in any of the cited references that teaches or suggest that the initializing of the S-box disclosed by Schneier occurs in a manner that is different form what is conventional in the prior art as described in Applicant's description of the the prior art and the applicant continued and discussed further that this system requires a substantial amount of CPU resources thereby severely restricting the CPU for other purposes." Thus applicant finally argued that for the reasons discussed above the independent claims 1 and 11 are now in condition for allowance.

Examiner disagrees with the above argument.

As far as the applicant disclosure is concerned, the state memory "316" is initialized with an incrementing pattern (ie., location 0 contains the value 0, location 1 contains the value 1 and so on.) [See Page 8, lines 4-7] and this is explicitly disclosed by **Schneier** as follows "Initializing the S-box is easy, first fill it linearly: S0=0; S1=1,....S255=255 Schnier does not discloses the necessity of the loading of the incrementing pattern from an external memory. The fact that the Memory is initialized with an incrementing pattern is explicitly taught by Schnier and the fact that the initialization is done with/ without loading the incrementing pattern from an external memory is design choice. One having ordinary skill in the art can easily implement the RC4 algorithm by initializing the incrementing pattern either with or without loading the incrementing pattern from an external memory. As far as the detail steps/processes by which the shuffling operation is executed as described in the applicant disclosure is concerned, it is neither described nor written in detail in the independent claims. In other words, the process of initializing in an incrementing pattern which is already described by the Schnier with loading the incrementing pattern from an external memory verses without loading the incrementing pattern from an external memory as the criterion of implementing the RC4 (ARCFOUR) encryption algorithm, is a matter of a design choice which can be performed by one of ordinary skill in the art and does not patentably distinguishes the claimed inventions from the references on the record. See St. Regis Paper Co. v.Bemis Co., Inc., 193 USPQ 8 (7TH Cir. 1977).

Applicant's second argument is again regarding the independent claims 1 and 11

The argument raised by the applicant is based on the comparison of the advantages that application provides over the reference on the record, namely Vano.

It is argued by the applicant that the there in nothing in reference on the record that teaches or suggest that the initializing of the S-box disclosed by the Schneier in particular that is different from what is conventional in the prior art. The applicant

assumed and concluded with out supporting evidence that, the reference on the record is implemented based on the CPU based encryption/decryption system which requires a substantial amount of CPU resources than the one offered by the presently claimed invention.

In response to the above assumption/argument by the applicant, the Examiner point out the following.

Advantages that could be provided by the invention over the prior art cannot be read into the claims. In fact, though the advantage of the invention is implicitly/inherently assumed to be described in the specification by the applicant, the specification is not the measure of the invention. Therefore, limitations contained therein/assumed to be contained therein cannot be read into the claims for the purpose of avoiding the prior art. (See In re Sporck, 55 CCPA 743, 386 F 2d 924, 155 USPQ 687 (1968))

Applicant's third argument is regarding the dependent claims.

Applicants argued that the since the independent claims are patentable therefore all the claims dependent namely claims 2-10 and 12-22 thereon are also in condition for allowance for the same reasons argued for the independent claims 1 and 11.

In response to the above argument by the applicant, the examiner response discussed to the independent claims 1 and 11 mentioned above is also valid towards this argument.

Therefore all the **elements of the limitations of claim 1-22** is explicitly or implicitly suggested and disclosed by the references on the records.

The rejections remains to be valid unless and otherwise the claims are further amended to introduce/include detail elements of the invention with out adding new matters and that are not taught/described/suggested/disclosed by the references on the record.

Claim Rejections - 35 USC § 103

5. **Claims 1-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over by Johns-Vano (hereinafter refereed as "**Vano**) (European Patent Publication No. "EP 0895164")(Publication date Feb 03, 1999) in view of a book by **Bruce Schneier:** Title "Applied Cryptography" " Chapter 17, "Other Stream Ciphers and Real Random-Sequence Generation" (hereinafter refereed as **Schneier**) (Pages 397-398)(both the references are submitted by the applicant and are included in the applicant IDS)

6. **As per claim 1 Vano** discloses a system for encrypting and decrypting data formed of a number of bytes using an encryption algorithm, [figure1, ref. Num "100" or "Cryptographic Engine"; "Abstract"; column 7, lines 22-29]

comprising:

- A system bus; [Figure 1, ref. Num "510" "Out Put bus"; column 4, lines 1-4]
- An encryption accelerator arranged to execute the encryption algorithm coupled to the system bus; [Figure 1, ref. Num "550"; figure 1; column 4, lines 1-4; column 8, lines 20-24] (An encryption accelerator met to be "Cryptographic co-processor" shown on figure 1, ref. Num "550"), the encryption accelerator including a state memory. (Figure 1, reference "554" or "state register"]
- A system memory [Figure 1, ref. Num "200" or ref. Num "202"];(Microcode memory shown on figure 1, ref. Num "200" and "202" is met "a system memory) coupled to the system bus arranged to store a secret key array associated with the data; [Column 4, lines 29-35; and column 8, lines 20-25] (As explained on column 4, lines 29-35 a channel program is loaded into the microcode memory

and on column 8, lines 20-24, it has been explained that a channel variable program can contain cryptographic encryption key") and

- A central processing unit (Figure 1, ref. Num "502";) (ALU is inherently an indication of the CPU since arithmetic logic unit, is the part of a computer that performs all arithmetic computations, such as addition and multiplication, and all comparison operations. The ALU is one component of the CPU (central processing unit) coupled to the system bus (Figure 1)

Vano does not explicitly disclose

- The state memory is initialized with an incrementing pattern without loading the incrementing pattern from an external memory.

However, in the same field of endeavor, **Schneier** discloses

- Storing of an incrementing pattern in the state memory array
- [Page 397, lines 23] (filling the s-box linearly)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the ARCFOUR or RC4 encryption algorithm including the features of initializing the state memory in an incrementing pattern with or without loading the incrementing pattern from an external memory as per teaching of Schneier into the configurable cryptographic processing engine and method as taught by **Vano** in order to provide a faster encryption.(It is known that encryption is fast about 10 times faster than DES, see page 397, line 22)

7. **As per claim 2 the combination of Vano and Schneier** discloses a system for encrypting and decrypting data as applied to claim 1 above. Furthemore **Vano** discloses the system wherein the encryption accelerator includes a state memory [Figure 1, reference "554"or "State register"] that includes a plurality of state memory values each of which is associated with a particular state memory location. [Column 6, lines 19-23]

8. **As per claim 3 the combination of Vano and Schneier** discloses a system for encrypting and decrypting data as applied to claim 1 above. Furthemore **Vano** discloses the system further comprising: a storage unit arranged to store at least a portion of the data to be encrypted [Figure 1, reference "564", date in register "564"; column 6, lines 44-47]

9. **As per claim 9-10 the combination of Vano and Schneier** discloses a system for encrypting and decrypting data as applied to claim 1 above. Furthemore **Vano** discloses the system further comprising an external memory [figure 1, reference "12"] coupled to the state memory arranged to store selected state memory values. [As explained in claim 1, about "channel program" see column 4, lines 29-33]

10. **As per claim 11,13-14, 21-22 Vano** discloses

- An encryption accelerator [Figure 1, ref. Num "550"] (An encryption accelerator met to be "Cryptographic co-processor" shown on figure 1, ref. Num "550") comprising:

- A combinational logic block arranged to perform a pre-determined logic operation on selected input values;[Figure 1, ref. Num "576" and column 6, lines

50-55) ("As explained on column 6, lines 50-55 a Permuter shown on figure 1, ref. Num "576" performs cryptographic operations as explained on column 6, lines 50-55)

- A state memory array[Figure 1, ref. Num "554" or "State Register"] arranged to store a plurality of state memory values;[Column 6, lines 19-22;] (state memory values is met "channel program states")

- A state machine coupled to the state memory array that directs performance of encryption algorithm.[Figure 1, ref. Num "558", "control register"; column 6, lines 31-36]

    - Performing a shuffling operations on the fly while concurrently retrieving a secret key associated with the data,[Column 6, lines 54-59; Column 6, lines 19-21; column 8, lines 20-24](Permuters select bits from state register as explained on column 6, lines 54-59 and the state register contains channel program as explained on column 6, lines 19-21 and the key is also contained in the channel program as explained on column 8, lines 20-24)

    - Byte-wise transferring the data to the combinational logic block as a first input value, and transferring a corresponding state memory value to the combinational logic as a second input value; logically operating on the first and the second input values by the combinational logic to form an encrypted data byte;[figure 1](As shown on figure 1, it is implicit to transfer data from the data register "564" and the state register "554" to the permuter which is shown on figure 1, ref. Num "576") and

- Outputting the encrypted data byte.[Figure 1, ref. Num "566", "data out register"]

Vano does not explicitly disclose

- Storing of an incrementing pattern in the state memory array without loading the incrementing pattern from an external memory

- Wherein the shuffling operation includes moving each of the plurality of state memory values based upon the secret key,

- Byte-wise transferring of data

However, in the same field of endeavor, **Schneier** discloses

- Storing of an incrementing pattern in the state memory array with/without loading the incrementing pattern from an external memory [Page 397, lines 23] (filling the s-box linearly)

- Wherein the shuffling operation includes moving each of the plurality of state memory values based upon the secret key.[Page 397, lines 23-page 398 line 3]

- Byte-wise transferring of data [Page 397, lines 21-23](S-box-entries are exclusively OR'd byte-wise with plaintext)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the ARCFOUR or RC4 encryption algorithm per teachings of **Schneier** into the configurable cryptographic processing engine and method as taught by **Vano** in order to

provide a faster encryption.(It is known that encryption is fast about 10 times faster than DES, see page 397, line 22)

11. **As per claim 4 and 12 Vano** discloses

- As many as two encryption algorithm may performed at the same time in the crytptographic engine. [see Abstract]

Furthermore Vano discloses that symmetric cryptographic alogorithm can be used. [Column 6, lines 53-54]

Vano does not explicitly discloses this particular the encryption algorithm is an ARCFOUR encryption algorithm./even though RC4 is known symmetric block cipher algorithm.

However, in the same field of endeavor, **Schneier** discloses

The importance of RC4 algorithm and stating that encryption in RC4 is fast, about 10 times faster than DES.[Page 397, lines 22]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of the ARCFOUR or RC4 encryption algorithm per teachings of **Schneier** into the configurable cryptographic processing engine and method as taught by **Vano** in order to provide a faster encryption.

12. **As per claim 5,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 4 above. Furthermore **Schneier** discloses the method wherein the system encrypts the data using the ARCFOUR algorithm by, and

shuffling each of the plurality of state memory values from an original state memory location to a corresponding shuffled state memory location based upon the secret key array[Page 397, lines 24- page 398, line 3].

13. **As per claim 6,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 5 above. Furthermore **Vano** discloses the system wherein the shuffling operation comprises: transferring the secret key array and an associated message data length into the encryption accelerator by way of the system bus thereby preserving central processing unit resources. [Column 6, lines 44-47]

14. **As per claim 7,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 6 above. Furthermore **Schneier** discloses the system wherein the shuffling is performed on the fly concurrently with the transferring.[Page 397] (fly byte-wise operation is a known technique in block cipher)

15. **As per claim 8,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 7 above. Furthermore **Vano** discloses the system further comprising: upon completion of the shuffling, the data (which is transferred from the register shown on figure 1, ref. "564"; column 6, lines 44-47] and **Schneier** discloses that the state memory that is exclusive OR'd with the byte of data to be encrypted.[Page 397, lines 21-23]

16. **As per claim 15-19,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 1 above. Furthermore **Vano** discloses an input latch and output latchs of the encryption acceleration.[figure 1; Column 6, lines 44-46](data in register shown

on figure 1, ref. Num "564"and the data out register shown on figure 1, reference "566" are met to be as the input and output latches of the encryption accelerator. The microsequencer 302 of the CPU) loads data into and from the registers as shown on Column 6, lines 44-46)

17. **As per claim 20,** the combination of **Vano** and **Schneier** discloses the system as applied to claim 1 above. Furthermore **Schneier** discloses the system wherein the accelerator further includes a first index counter and a second index counter . [Page 397, lines 14-page 398 line 10]

Conclusion

18. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.

07/20/2005

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100